file I can produce vote counts for each iVotronic, each ballot style, each precinct, and each race.

36.   Finally, I examine one of several "results" files that are produced by the Unity software. From this I can determine for each precinct and each race the number of iVotronic votes recorded from the PEBs, the number of votes that might have been recorded by reading directly from the memory cards, and the number of paper or absentee ballots. (If the county chooses not to print this information, it might not appear.)

37.   My programs count votes at the precinct/iVotronic/ballot style/race level, votes from the "vote cast" codes, and votes from the results file. Discrepancies between these files usually indicate that procedures have not been followed. I verify that iVotronics used for voting have been closed and that the PEB used for closing shows up in the system log file as having the correct number of votes uploaded. I verify that all the memory cards have been collected and their data uploaded, and I identify instances in which the ballot definitions in Unity differed from those in the iVotronics. I also record lists of the events in the event log that indicate that the machines have been malfunctioning and thus might not be recording votes correctly or might not have recorded the correct data, although I am not able to determine what the incorrect entries might be.

38.   I have over the course of four General Elections now seen instances of probably all the different errors that could occur. Assuming there is a record in these files of any of the hardware by serial number, then my programs will detect an inconsistency and report that in an EXCEPTIONS file.

12

Conclusion: A Forensic Audit Is the Only Way to Have Confidence in the Vote Tally

29.   For the reasons stated above, the electronic voting systems in place in Pennsylvania (including Allegheny County) are unreliable and vulnerable to attack. That is why other jurisdictions have discontinued the use of some electronic voting machines.

30.   There were well-publicized attacks on America's voting infrastructure this year by foreign agents and other hostile forces, attacks confirmed by the United States' government's security agencies.

31.   Given this reality, and given the vulnerability of the electronic machines used here, it is crucial that computer experts be able to forensically evaluate the electronic voting data from Allegheny county to ensure that the vote was counted accurately.

32.   I affirm that the foregoing is true and correct.

_____   2 Dec 2016
DUNCAN BUELL   Date

Sworn before me this 2nd day of December, 2016, in Columbia, SC

_____
NOTARY PUBLIC

13

AFFIDAVIT OF J. ALEX HALDERMAN

J. ALEX HALDERMAN, being duly sworn, deposes and says the following under penalty of perjury:

1.   My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Affidavit in support of the petitioners.

2.   I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

3.   My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, data privacy, and electronic voting.

4.   I have authored more than seventy articles and books. My work has been cited in more than 4,700 scholarly publications. I have served on the program committees for thirty research conferences and workshops, and I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938 E Award for teaching and scholarship.

5.   I have published peer-reviewed research analyzing the security of electronic voting systems used in Pennsylvania, other U.S. states, and other countries. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom" review of the state's electronic voting systems. I have also investigated methods for improving the

security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records.

6.   My full curriculum vitae, including a list of honors and awards, research projects, and publications, is attached as Exhibit A.

Context: Cyberattacks and the 2016 Presidential Election

7.   The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John Podesta, the chairman of Secretary Clinton's campaign. Exhibits B and C. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. Exhibit D. The Department of Homeland Security has stated that senior officials in the Russian government commissioned these attacks. Exhibit E. Attackers attempted to breach election offices in more than 20 other states. Exhibit F.

8.   Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote-counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that could have caused the wrong winner to be announced. Exhibit G. Countries other than Russia also have similarly sophisticated cyberwarfare capabilities.

9.   If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices (or the offices of election service vendors) well in advance to find ways to break into the computers. Next, closer to the election,

when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines in some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling.

The Vulnerability of American Voting Machines to Cyberattack

10.   As I and other experts have repeatedly documented in peer-reviewed and state-sponsored research studies, American voting machines have serious cybersecurity problems. Voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. As I have demonstrated in laboratory tests, in just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote.[1]

11.   Whether voting machines are connected to the Internet is irrelevant. Sophisticated attackers such as nation-states have a developed a variety of techniques for attacking non-Internet-connected systems.[2] Shortly before each election, poll workers copy the ballot design from a regular desktop computer in a government office (or at a company that services the voting machines) and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers infect that computer, they can spread vote-stealing malware to every voting machine in the area.

---

[1] A video documenting this result is publicly available at https://youtu.be/aZws98jw67g.

[2] A well known example of this ability, which is known as "jumping an airgap", is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Most voting machines also have reprogrammable software ("firmware") that can in many cases be manipulated well in advance of the election to introduce vote-stealing malware. Technically sophisticated attackers can accomplish this with ease.

12.   While the vulnerabilities of American voting machines have been known for some time, states' responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Pennsylvania, continue to use out-of-date machines that are known to be insecure.

13.   Procedural safeguards used by Pennsylvania and other states to protect their voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack. These inadequate safeguards include tamper evident seals, protective counters, and test decks.

14.   Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers. The types of seals typically used for voting equipment can be bypassed without detection using readily available tools.[3] For some seals, these include screwdrivers and hair dryers. By bypassing the seals, an attacker with physical access to the voting machines can modify their internal programming to make them output fraudulent results.

15.   Malware installed on a voting machine can subvert the protective counter by changing its value in the machine's computer memory. Malware can subvert test decks by refraining from cheating when only a small number of ballots have been scanned (as is the case when a test deck is used), or by only cheating at a specified time of day (electronic voting machines typically have internal clocks).

---

[3] https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf

Pennsylvania's Voting Machines Are Among The Most Vulnerable In The U.S.

16.   Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks.

17.   More than 70% of American voters have their votes recorded on some form of paper, which provides permanent evidence of their intent in the event of a post-election recount. In Pennsylvania, less than approximately 20% of votes are cast using paper ballots or voter-verified paper audit trails. The remaining approximately 80% are cast on paperless direct-recording electronic (DRE) computer voting machines that do not create a paper record of each vote.

18.   Paperless DRE voting machines have been repeatedly shown to be vulnerable to cyberattacks that can change or erase votes, cast extra votes, or even infect the software used to tabulate results. Since paperless DREs do not generate a physical record of the vote, these attacks may be difficult or impossible to detect or to reverse. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.

19.   To my knowledge, there are six models of DREs presently in use in Pennsylvania. Every one of these models has been examined by security researchers (in some cases, repeatedly), and all have critical security vulnerabilities that could be exploited by attackers to alter the outcome of elections. These vulnerabilities include architectural weaknesses that cannot be repaired through software updates. As a result, every DRE in use in Pennsylvania is vulnerable to cyberattacks.

20.   The vulnerable DREs used in Pennsylvania include:

21. **Hart InterCivic eSlate** — This model of machine was examined by security experts

as part of the California "Top to Bottom" election technology review[4] and the Ohio

EVEREST election system security review[5]. Both studies found significant

vulnerabilities, and California subsequently decertified the machine.[6] The memory cards

used by eSlates to transfer votes to a central counting computer are vulnerable to

undetectable tampering. The internal security mechanisms of the machines are easily

defeated, enabling malicious software to change or erase votes, cast extra votes, or

modify the eSlate's software or the software of the JBC, the machine used to tabulate

votes. These vulnerabilities could allow attackers to compromise large numbers of

machines and alter the election outcome.

22. **Sequoia (Dominion) AVC Advantage** — This model of machine has been studied

by multiple groups of security researchers. I have extensively analyzed the AVC

Advantage, and I published a peer-reviewed security study of the machines in 2009. My

study demonstrates that malware can infect the machines and alter votes. Such malware

can spread to the machines via the removable memory cartridges that are used to program

the ballot design and offload votes.[7] My research additionally shows that such malware

can defeat all of the hardware and software security features that are used by the

machines. A separate group of researchers performed a security review that also

concluded the AVC Advantage has significant vulnerabilities, including that it would be

---

[4] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/hart-amended-recert-final-120707.pdf
[5] http://www.patrickmcdaniel.org/pubs/everest.pdf
[6] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/hart-amended-recert-final-120707.pdf
[7] https://jhalderm.com/pub/papers/avc-evt09.pdf

straightforward to install vote-stealing malware by replacing one firmware chip.[8]

Deficiencies of this voting machine are not limited to security vulnerabilities: in the 2008

New Jersey Republican primary, 37 of these machines exhibited a software bug in which

the number of votes recorded was higher than the number of voters.[9]

23. **Danaher Shouptronic 1242** — This model of machine was introduced in 1984 and

has not had its security features updated in more than 30 years. Cyberattacks have

become significantly more sophisticated during that time, and the security features in the

machine are unlikely to be able to defend against today's attackers. Researchers at

Lehigh University have analyzed the Shouptronic's computer architecture and shown that

it is constructed in a very similar manner to the AVC Advantage.[10] This computer

architecture subjects the machines to many of the same attacks. Attackers can replace the

machines' ROM chips to cause the machines to output fraudulent results. The machines'

design makes it extremely likely that malware can infect the machines via the removable

memory cartridges that are used to program the ballot design and retrieve vote totals. The

Shouptronic has also already been problematic in past elections,[11] malfunctioning and

causing significant delays in voting multiple times in Pennsylvania, Tennessee, and Ohio.

24. **Premier/Diebold (Dominion) AccuVote TSX** — I performed a security analysis of

the AccuVote TSX as part of the California Top-to-Bottom review[12], and the machine

was also studied as part of Ohio's Project EVEREST[13] and by independent security

---

[8] https://mbernhard.com/advantage-insecurities-redacted.pdf

[9] https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/appel.pdf

[10] https://verifiedvoting.org/downloads/2008Danaher1242-full.pdf

[11] https://w2.eff.org/Activism/E-voting/infosheets2006/ELECTronic1242.pdf

[12] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf

[13] http://www.patrickmcdaniel.org/pubs/everest.pdf

researchers[14]. All of these studies found extremely serious security problems. This machine, along with its predecessor the AccuVote-TS, which I studied extensively in a 2007 security review[15], can be exploited by attackers to alter election results. The security features built into the machines are inadequate to defend against cyberattacks, and vote-stealing malware can spread on the machines' removable memory cards. If attackers infect counties' election management system computers, the attacker can spread vote-stealing malware to every voting machine in the county. Moreover, these machines rely on Windows CE as their operating system, software that has not been supported by Microsoft in several years,[16] and has been shown to have significant vulnerabilities itself, beyond those of the election-specific software.[17] A local attacker with physical access to the machines can additionally tamper with them by manipulating the machines' removable memory cards. Access to these cards is protected using a low security lock that can be picked using only a BIC pen.[18] California decertified the Accuvote TSX in 2007.[19]

25. **Sequoia (Dominion) AVC Edge** — Also decertified by California in 2007,[20] this machine has vulnerabilities similar to those of the TSX and the eSlate. In the California Top-to-Bottom review, security experts found that remote attacks could spread malware to the machines and change, steal, or add votes. Furthermore, such malware can persist even if election workers reinstall an uncorrupted version of the election software. The

---

[14] http://www.blackboxvoting.org/BBVtsxstudy.pdf

[15] http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06EVT.pdf

[16] https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Windows%20CE%20.NET%204.0

[17] https://www.cvedetails.com/product/1079/Microsoft-Windows-Ce.html?vendor_id=26

[18] Shown in this video demonstration: https://www.youtube.com/watch?v=vqNJL0fYwSk

[19] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf

[20] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-100109.pdf

California study further discovered that malicious software on the machines could conceal vote-tampering from pre-election testing, hiding manipulation of votes and making the machine output appear otherwise normal. The election software running inside the AVC Edge can also be tampered with by a local attacker with physical access to the machine by replacing a memory card inside the machine's case. I demonstrated this vulnerability by hacking one AVC Edge to make it run the arcade game Pac-Man.[21] A real attacker could just as easily modify the software to make the machine cheat in elections.

26. **Election Systems & Software iVotronic** — The iVotronic was studied by security experts as part of Project EVEREST.[22] The investigation found that firmware on these machines contained buffer overflow vulnerabilities, which could be exploited to infect the machines with malware and alter the election outcome. Further vulnerabilities in the machines include that the Personalized Electronic Ballot module (PEB), which is used to program the ballot design before the election, had only trivially circumventable security protections. The EVEREST researchers also found that the cryptographic keys used by the machines to encrypt votes could be easily extracted by attackers, who could then read or manipulate the vote data.

Examining the Physical Evidence is the Only Way to Ensure the Integrity of the Election

27.   One explanation for the results of the 2016 presidential election is that cyberattacks influenced the result. This explanation is plausible, in light of other known cyberattacks intended to affect the outcome of the election; the profound vulnerability of American voting

---

[21] https://jhalderm.com/pacman/
[22] http://www.patrickmcdaniel.org/pubs/everest.pdf

machines to cyberattack; and the fact that a skilled attacker would leave no outwardly visible evidence of an attack other than an unexpected result.

28.   The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, the paper ballots (where available), paper audit trail records (where available), and the voting equipment itself.

For DREs With Paper Trails, The Paper Trail Must Be Recounted By Hand

29.   For DRE voting machines that generate paper vote records (VVPAT records), the paper must be examined in order to detect potential cyberattacks. Simply commanding the machines to output the vote totals again would not reliably uncover an attack. This is because any attack on the machines during the election would likely have changed the digital record of the votes stored in the voting machines' memory (as well as in any external memory cartridges or cards). Therefore, the digital records do not reliably preserve voters' intent. In contrast, a manual examination of the VVPAT record would expose this style of cyberattack.

For DREs Without Paper Trails, A Forensic Examination Must Be Conducted

30.   Most of Pennsylvania's votes are recorded on DRE voting machines that do not generate any paper record of the individual votes. The only way to reliably determine whether the election outcome on these machines was changed by a cyberattack is to forensically examine the election equipment. A complete forensic examination would include examining the machines' hardware and software, their removable media, and the election management system computers used to program the machines and aggregate election results.

31.   Forensic examination could reveal evidence of an attack, such as successful attempts to spread malware to the machines. Such evidence could include malware itself, signs of remote intrusion in the election management system, or indicators that digital vote records or other files

were manipulated or deleted. If a forensic examination can determine the manner in which the machines were compromised, it might also allow manipulation of the election result to be corrected.

For Optical Scan Paper Ballots, The Ballots Must Be Recounted By Hand

32.   For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, is necessary to reliably detect possible hacking. Using optical scan machines to conduct the recount, even after first evaluating the machines through a test deck, is insufficient to detect potential cyberattacks. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests.[23]

33.   If the optical scanners were attacked by infecting them with malware, such malware might still be active in the scanners during the recount. Recounting the ballots using an infected scanner would likely yield the same results as the original count, despite the results being wrong. If attackers managed to compromise the count during election day but in a manner that did not persist on the machines, machine recounts would still be insufficient. Attackers who were able to infect the machines before the election likely would be able to attack them again, perhaps using the same methods, prior to the recount. The dates and the procedures of the recount are widely publicized, so attackers would know when to strike. This would result in the scanners producing the same incorrect results when the ballots were scanned again.

34.   In contrast to machine recounts, a manual recount, where the paper ballots are inspected by humans, can reliably detect any cyberattack that might have altered the election

---

[23] Volkswagen used a similar strategy to conceal the way it circumvented EPA emissions tests: http://www.reuters.com/article/us-volkswagen-emissions-audi-idUSKBN1370Q3

outcome on the optical scanners. A manual recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference.

35.   Manual recounts are not necessarily more time-consuming than recounting using optical scanners, particularly when only one race is being counted. A manual recount focuses on a single contest, and human observers typically proceed by sorting the ballots into stacks according to the chosen candidate and then counting the ballots in each stack. This is an efficient and straightforward process. If scanners are used, the scanners must be programmed and tested, new removable media must be located and programmed, and the ballots must be fed into the scanner by humans. These steps are not necessary when hand counting is used.

36.   The paper ballots used in Pennsylvania can be counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether the voter intended to make a mark. Pennsylvania's optically scanned paper ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted efficiently and accurately in a manual recount.

37.   Examining the available physical evidence, including paper ballots, paper vote records, and the voting equipment itself, will set a precedent that will provide an important deterrent against cyberattacks on future elections. By performing a rigorous recount now in a method that would detect cyberattacks affecting the outcome (that is, by thoroughly examining this physical evidence), we send a strong signal to attackers that any future computer-based tampering efforts are likely to be caught.

This affidavit was executed on the 30th day of November, 2016 in Ann Arbor, Michigan.

_____
J. ALEX HALDERMAN

Sworn to before me this 30th day of November, 2016.

_____
Notary Public

My Commission Expires: 04-04-2018

TOBIN C. DARNELL
NOTARY PUBLIC, STATE OF MI
COUNTY OF WASHTENAW
MY COMMISSION EXPIRES Apr 4, 2018

AFFIDAVIT OF HARRI HURSTI

I declare under penalty of perjury under the laws of Pennsylvania that the following is true and correct.

1. I submit this Affidavit in support of petitions to recount/recanvass the vote in Montgomery County, Pennsylvania.

2. I have been a consultant and a co-author of several studies commissioned or funded by various U.S. states and the federal government on computer security. In the area of election security, I am the co-author of several peer-reviewed and state-sponsored studies of election system vulnerabilities. Most notably, I was a co-author of the EVEREST comissioned by the Secretary of State of Ohio (http://hursti.net/docs/everest.pdf), a study of vulnerabilities in Sequoia AVC voting machines (http://hursti.net/docs/princeton-sequoia.pdf), and a study of the Estonian Internet voting system (http://hursti.net/docs/ivoting-ccs14.pdf). In 2005, I developed the Hursti Hack(s), a series of four tests in which I demonstrated how voting results produced by Diebold Election Systems voting machines could be altered. I have served as an expert on electronic voting issues in consultations to officials, legislators, and policy makers in five countries. I received the Electronic Frontier Foundation's EFFI Winston Smith Award in 2008, and the Electronic Frontier Foundation EFF Pioneer Award in 2009 for my research and work on election security, data security and data privacy. I recently founded Nordic Innovation Labs to advise governments around the world on election vulnerabilities. My qualifications and experience are further detailed at the following website:

https://nordicinnovationlabs.com/team/harri-hursti/.

How AVC Advantage Machines Work

3.   According to VerifiedVoting.org,[1] Montgomery County uses direct recording electronic ("DRE") voting machines called Sequoia AVC Advantage. I have studied these machines in detail, including for a report submitted to the New Jersey Supreme Court.

4.   With respect to all DRE machines, including the AVC Advantage, the voter indicates a selection of candidates via a user-interface to a computer; the program in the computer stores data in its memory that (are supposed to) correspond to the indicated votes; and at the close of the polls, the computer outputs (what are supposed to be) the number of votes for each candidate.

5.   For the AVC Advantage, electronic ballot definitions are prepared and results are tallied with a Windows application called "WinEDS" that runs on computers at election headquarters in each county. Ballot definitions (contests, candidate names, party affiliations, etc.) are transmitted to the Advantage via a "results cartridge," which is inserted at the election warehouse before the machines are transported to polling places before the election. The votes cast on an individual machine are recorded in the same cartridge, which poll-workers bring to election headquarters after polls close.

6.   The AVC Advantage 9.00 includes an "audio kit" containing its own computer board. Any voter who wishes to vote by audio instead of on the large printed buttons-and-lights voter panel is permitted to do so. Voters might wish to vote by audio because of vision impairments, mobility impairments, inability to read, or for any other reason; indeed, voters are not required to state the reason they wish to vote by audio.

---

[1] https://www.verifiedvoting.org/verifier/#year/2016/state/42/county/91.

7. The audio-kit computer resides on a "daughterboard" inside the cabinet but separate from the main circuit board of the AVC Advantage (which is called the "motherboard").

8. Unlike the motherboard firmware, the firmware of the daughterboard does not reside in read-only memory ("ROM"). It resides in "flash memory"; the flash memory contains the election control program, as well as ballot definitions and other files. Unlike ROM, which cannot be modified without removing and replacing physical computer chips, flash memory can be written and rewritten by the software (or firmware) inside the computer.

AVC Advantage Machines Are Vulnerable and Not Reliable

9. Our study of the AVC Advantage machines found that the AVC Advantage is vulnerable to election fraud, via firmware replacement and other means. Even in the absence of fraud, the AVC Advantage has user interface flaws that could cause votes not to be counted.

10. As we explained in our report, the AVC Advantage is easily "hacked" by tampering with the machine's firmware. Because there is no paper receipt, all electronic records of the votes are under control of the firmware, which can manipulate them all simultaneously.

11. Without even touching a single AVC Advantage, an attacker can install fraudulent firmware into many AVC Advantage machines by viral propagation through audio-ballot cartridges. The virus can steal the votes of blind voters, can cause AVC Advantages in targeted precincts to fail to operate; or can cause WinEDS software to tally votes inaccurately.

12. AVC Advantage Results Cartridges can be easily manipulated to change votes, after the polls are closed but before results from different precincts are cumulated together.

13. The vulnerability of the machines means that good-faith programming errors can also manipulate votes, even without malicious intent. The outdated software renders the machines prone to errors that could affect vote totals.

14. There are also major user interface flaws that may cause inaccuracy in counting votes, including that the AVC Advantage sometimes appears to record a vote when in fact it does not, and vice versa.

These DRE Machines Are Susceptible to Fraud and Tampering

15. The AVC Advantage machines are vulnerable to fraud and inadvertent tampering in a variety of ways. Specifically, the daughterboard and the WinEDS system renders them particularly vulnerable to tampering, fraud, and virus infection.

16. For example, as described above, in addition to the Z80 computer on the AVC Advantage motherboard, the AVC Advantage version 9.00 contains a second computer, called the daughterboard, which is used in audio voting.

17. One can install fraudulent firmware into the daughterboard simply by inserting an audio-ballot cartridge infected with a virus into the slot in the daughterboard. An honest elections official who is unaware of the presence of the virus can do this unwittingly. The process takes one or two minutes. One virus can propagate onto all the WinEDS computers and AVC Advantage voting machines used in a county. This is a very severe vulnerability.

18. Fraudulent firmware in the daughterboard can steal the votes of blind voters, or of any voters who use audio voting, and can selectively cause voting machines to fail on election day in precincts chosen by the attacker.

19. On the version 9 AVC Advantage, the daughterboard does not directly write votes to the Results Cartridge. The motherboard controls the Results Cartridge, and communicates with the daughterboard via messages sent through a cable. When a voter votes using audio, the daughterboard presents the ballot aurally to the voter, and communicates candidate selections to the motherboard.

20. Audio voters use an input device that is connected to the daughterboard, not the motherboard. Thus it is very easy for fraudulent daughterboard firmware to steal the votes of audio voters, simply by conveying different candidate choices to the motherboard. The votes of disabled voters are even more at risk, on the AVC Advantage, than the votes of those who use the full-face voter panel.

21. In addition, the attacker can cause voting machines to fail in a selected set of precincts. For example, if he disables a dozen or two voting machines in heavily populated districts across the state, then long lines of voters may form, and some voters may leave the polling place before voting. The significance of doing this attack via a daughterboard virus is that a single person can disable voting machines in hundreds of precincts that he chooses, without ever going near any of those machines.

22. To do this, the attacker then programs an audio-ballot virus, replacing the audio-voting software on the daughterboards of all AVC Advantage voting machines in the county.

23. On election day, when each machine is turned on, one of the first things that the motherboard does is to send a message to the daughterboard saying (paraphrase) "load the audio ballot," and the daughterboard normally responds saying (paraphrase) "OK." However, the

fraudulent daughterboard software responds with a different message, either one of the

following:

> • "Cannot load ballot." Then the AVC Advantage (motherboard) will display
>
> an error message on the Operator Panel, and the election cannot start.
>
> • A specially crafted message that triggers a buffer overrun bug. This causes the machine
>
> to reboot, in an infinite loop, or for as many repetitions as the daughterboard chooses.

In either case, the AVC Advantage will fail to start up on the morning of election

day, or will be delayed for a chosen number of minutes.

24. The audio-ballot cartridge loaded in the daughterboard contains the name and number of

the election district in which the machine will be used. Thus the daughterboard firmware has

enough information for an attack on specific precincts. This allows a selective denial of service

to specific demographic groups.

25. This general means of manipulating elections is well understood. In Ohio in the 2004

Presidential election, it was widely reported in the press that the misallocation of voting

machines led to unprecedented long lines that disenfranchised scores, if not hundreds of

thousands, of voters. Selective disabling, instead of misallocation, could produce a similar result.

26. The daughterboard virus is a very elementary attack. Virus programming is not much

taught in schools, but unfortunately there are many practitioners of it nonetheless. The number of

known computer viruses is enormous. The virus definition file maintained by the virus detection

firm Symantec lists over 17 million separate virus "signatures."

27. For this particular virus programming, not even a bachelor's-degree level of skill is

necessary. The daughterboard is an Intel-486-compatible computer running a DOS operating

system—just like the hardware and software of the IBM PCs from about 1990. Millions of PC users gained familiarity with its scripting tools that would be helpful in creating viruses for the AVC Advantage daughterboard.

28. We found that it is also possible to reverse-engineer the daughterboard firmware. The daughterboard computer is made by Compulab. We were able to find documentation for this computer on the Internet. Compulab sold this computer for many applications, not just voting machines, and development tools are available for it. Using these development tools, an attacker could extract the firmware and reverse-engineer it. Then, using the results of this analysis, he could devise fraudulent firmware of the kind we described above.

29. The motherboard is also vulnerable to malicious daughterboard firmware. One might hope that disabling audio voting would make the motherboard immune to harmful effects from a daughterboard virus. Unfortunately, this is not the case. Because of a mistake Sequoia made in programming the motherboard firmware, the AVC Advantage is vulnerable even if the ballot definition says not to use audio voting.

30. In addition to the daughterboard, the WinEDS system is vulnerable to fraud and tampering. Election workers prepare ballots for the AVC Advantage on WinEDS computers at the election warehouse, or at the board of elections, or other locations. The electronic ballot definition loaded into the Results Cartridge specifies not only the names of the candidates, but several other options about the election. In preparing a ballot definition for the AVC Advantage, one can choose the option to disable audio voting. The (large-format) Results Cartridge with this option setting is then loaded into the (motherboard of the) of the AVC Advantage. This tells the motherboard not to use the daughterboard.

31. The WinEDS election-management software is known to be insecure, based on studies done by the State of California. In our examination we noticed some of the same weaknesses in WinEDS that were previously reported elsewhere.

32. In summary, AVC Advantage voting machines and WinEDS vote-tabulation software are both severely vulnerable to viruses that can alter election results. We have demonstrated the feasibility of creating a computer virus that propagates from AVC Advantage machines to each other, and to WinEDS computers. Such a virus can carry payloads that modify votes inside the AVC Advantage, and modify election and vote databases in WinEDS. The virus can also be programmed to erase itself from voting machines just before the polls close, so as to avoid detection after the fact.

Without A Forensic Evaluation It Is Impossible To Whether the Original Tally Can Be Trusted

33. Because of these numerous vulnerabilities, a full forensic evaluation by independent experts of all of the component's of Montgomery County's Sequoia voting system used in the 2016 presidential general election is the minimum requirement to have any trust at all that the vote was accurately recorded and tallied. This includes:

      a.   Every computer on which Sequoia's WinEDS software was used during the election cycle to prepare Montgomery County's electronic ballot definitions and audio ballots and tabulate results;

      b. A randomly selected sampling of Sequoia AVC Advantage electronic voting machines, with audio-ballot kits installed and on which ballots were cast. At a

minimum, a randomly selected sample of audio-ballot cartridges and results

cartridges; and

c. The audio ballot cartridge and results cartridge used for those Sequoia Advantage

machines.

34. Without such a forensic evaluation, there can be no confidence in the election results.

35. Simply instructing the WinEDS computer to display or print out the results will

accomplish nothing. The result will necessarily be identical to the initial computation. This

achieves nothing by way of verifying the accuracy or integrity of the results.

36. Similarly, re-uploading the results stored on the results cartridges from the Sequoia AVC

Advantage machines used in the election to the WinEDS computer would be an empty exercise.

Absent intervening tampering, the results stored electronically on each cartridge will be the same

as they were at the time of the initial upload.

37. By contrast, forensic examination by independent experts of the audio-ballot cartridges

inside one or more of the AVC Advantage machines used in the election could produce evidence

that the software resident on the cartridges had been infected with a virus capable of switching

votes from one candidate to another or rendering the affected AVC Advantage machine

inoperable on Election Day. It may then be possible to demonstrate the precise nature of any

vote-switching routine and its corrupting effect on the recording of votes for a candidate other

than the one intended by the voter.

40. Forensic examination of the WinEDS computer used by the county could produce

evidence that the WinEDS election management software installed on the computer had been

tampered with. Such tampering could be accomplished through direct physical access to the computer, connection of the computer to the Internet at any time before the election, or infection by a virus on one of the audio ballot cartridges that had been connected to the WinEDS computer for programming.

Executed on the 30th day of November, 2016 in Helsinki, Finland.

HARRI HURSTI